Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

SE PROTEGER DES CRYPTOLOCKERS ET RAMSOMWARES

QU'EST-CE QU'UN CRYPTOLOCKER ?

Le CryptoLocker est un logiciel malveillant de type « ransomware » qui se propageait, jusqu'à présent par un courrier électronique contenant une pièce jointe fichier .exe (ou zippé) caché sous un document, PDF, Word ou Excel (la liste est longue) ou un lien permettant le téléchargement de ce même fichier. A l'ouverture de ce fichier par l'utilisateur, Cryptolocker s'installe sur le poste, et peut dans certains cas ne pas être détecté par l'antivirus.
Pour rappel, un antivirus fonctionne sur la notion de liste noire, et protège uniquement contre ce qu'il connait (les signatures) ainsi que les variantes pour lesquelles des sommes de comportements anormaux permettent une détection.

Cryptolocker travaille en tâche de fond de façon imperceptible et à l'issu d'un certain temps (~5 à 15 min), certains types de documents sur les disques internes ou les partages réseau sont chiffrés et deviennent donc illisibles par l'utilisateur. Un message des pirates demande alors le paiement d'une rançon en ligne dans un court délai (généralement 72 heures au-delà desquelles les documents seront définitivement perdus), en échange de la fourniture de la clef de déchiffrement des données. Attention, d'autres formes de propagation de ce ransomware existent : caché dans des versions de logiciels/jeux piratés téléchargés sur Internet ou suite à une infection par des malwares de type « cheval de Troie » contractée sur des sites de mauvaise réputation ou infectés.

Chaque jour les pirates améliorent les attaques, nous constatons de fausses adresses emails utilisant le nom de domaine de votre société ou de partenaires connus.

Un ver informatique est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il a la capacité de se dupliquer une fois qu'il a été exécuté. Contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables.

Depuis le mois de Janvier 2020 notre service cyber Sécurité a constaté une recrudescence des attaques et une nouvelle forme d'attaque : Les pirates utilisent les failles de sécurité pour pénétrer le réseau local (Port 3389 ou autre ouverts, postes en Windows 7, poste sans mot de passe etc…). Une fois sur le réseau, un ver est introduit. Celui-ci va enregistrer les frappes claviers des collaborateurs. Grace à un logiciel d'intelligence artificiel, les pirates vont détecter les séquences claviers correspondant à la frappe de Login suivi de MDP (mot de passe). Lorsque les pirates connaissent tous les mots de passe utilisateurs, messageries, administrateurs, (pire) sauvegarde etc…. Tout est prêt pour une attaque terrible et foudroyante. La mise en place d'un logiciel de chiffrement (Cryptolocker). Toutes les données sont chiffrées ainsi que les sauvegardes. Il ne reste plus aux pirates qu'à demander une rançon.

COMMENT CA MARCHE ?

- **1er cas**

Une fois installé sur la machine de la victime CryptoLocker utilise son algorithme de génération de noms de domaine pour identifier le ou les serveurs de commande et de contrôle (C&C) avec lesquels il va pouvoir communiquer. Lorsqu'il a identifié son serveur C&C (cette opération peut durer environ 5 min), CryptoLocker lui demande la génération d'un couple de clés RSA 2048 bits. La clé privée reste sur le serveur tandis que la clé publique est envoyée au ransomware pour qu'il crée sa nouvelle clé de chiffrement qu'il utilisera pour chiffrer les différents fichiers. Quand il aura fini, Cryptolocker communique au serveur C&C l'achèvement du chiffrement : le message de demande de rançon apparait alors à l'écran.
C'est durant la 1ère phase de recherche du serveur C&C que l'on peut intervenir pour bloquer Cryptolocker en coupant toute communication Internet, soit environ 5 à 15 min pour les versions

actuelles, après il sera trop tard ! Cryptolocker met en œuvre des techniques de chiffrement robustes contre lesquelles aucun moyen simple de déchiffrement n'est actuellement connu.

2ème cas

Dernièrement, nous avons constaté que la clé de chiffrement était saisie manuellement ou avec un horodatage. Ce qui évite au cryptolocker de communiquer avec son serveur de chiffrement. La parade est quasi impossible à mettre en place. Il convient de protéger fortement son réseau pour empêcher le pirate de s'introduire dans le réseau local.

COMMENT SE PROTEGER

Les bonnes pratiques de protection :

A) Les collaborateurs

L'une des premières mesures est l'information et la sensibilisation des utilisateurs aux risques associés aux messages électroniques, fichiers attachés et/ou téléchargés et liens internet. On ne le répétera jamais assez, la principale mesure préventive reste du côté de l'utilisateur ! Ce type d'infection peut être facilement évité si les utilisateurs suivent ces 4 consignes de prudence élémentaire très efficaces :

- Ne jamais ouvrir un courrier électronique suspect (sujet, langue, syntaxe, sans rapport avec votre activité) ou de provenance douteuse (expéditeur inconnu) => le signaler à l'administrateur sécurité
- Ne jamais cliquer sur un lien web dans un courrier électronique non sollicité ou de provenance douteuse,
- Supprimer immédiatement chaque courrier électronique suspect ou de provenance douteuse.
- Ne jamais double-cliquer sur des documents en pièce attachée de courrier d'expéditeurs inconnus ou suspects, de type exe, zip ou avec un nom trop long pour voir l'extension. Ne jamais télécharger et installer des exécutables sans avis de l'administrateur, zip (logiciels, utilitaires, jeux…), notamment à partir de sites web douteux.

B) Sécurité générale (administrateur) :

- - Protéger son réseau local par un **Firewall puissant,** de dernière génération associée à des services de protection **mis à jour en permanence**.
- - Installer sur chaque machine un agent **antivirus** et préférablement une suite de sécurité de poste et le maintenir à jour : vérifier qu'il reçoit bien les dernières mises à jour de signatures plusieurs fois par jour.
- - Déployer une solution de protection de messagerie (en passerelle ou sur le serveur) pour contrôler le trafic de messagerie entrant : **anti-spam**, anti-phishing, anti-virus, filtrage du contenu : blocage des pièces attachées de type exécutables et doubles extensions, Zip avec mot de passe, ou fichier chiffré.
- Mettre en place une solution de protection de la navigation Internet : filtrage WEB : bloquer les catégories de sites non professionnels, suspects, illégaux ou dangereux, pour éviter les risques infections et accès en fonction de la réputation du site.

- Analyser les téléchargements avec un anti-virus en passerelle. Bloquer les téléchargements de fichiers exécutables, zippés avec un mot de passe ou chiffrés ; analyser et filtrer les flux Https et FTP. Bloquer ou limiter les autres communications : médias sociaux, notamment les transferts de fichiers.
- Maintenir les systèmes d'exploitation et les logiciels à jour, en appliquant les correctifs de sécurité et les patchs les plus récents.
- Activer les mécanismes de contrôle d'applications afin de vous assurer que seuls les logiciels validés par votre entreprise et dont vous assurez l'application des correctifs soient installés et exécutés.
- Activer ou mettre en place des systèmes de contrôle des périphériques amovibles (clés USB, disques externes, ...) afin de réduire le risque d'infection par ce vecteur.

Malgré les bonnes pratiques de sécurité, une infection peut tout de même survenir. Il vous sera, alors, nécessaire de recouvrer les données qui auront été chiffrées, sans payer de rançon car financer les pirates les aident à améliorer les Cryptolocker pour les rendre encore plus rentable.

A cet effet :

- Effectuer des sauvegardes régulières de vos données et les stocker sur des médias **non connectés en permanence au réseau** (afin qu'elles ne risquent pas d'infection) (Sauvegarde externalisée) : en cas d'infection de type ransomware vous retrouvez vos données en clair sur vos disques ou stockage mis à l'abri ou dans le Cloud.
- Ne pas laisser son disque dur externe ou serveur Nas constamment branché à son ordinateur ou au réseau. - Faire preuve de prudence lors de l'utilisation et d'échange de clés USB : installer un module contrôle des périphériques pour interdire l'exécution sur les périphériques de type clef USB ou disque amovible
- Au niveau du serveur il convient d'utiliser une solution logicielle et matérielle permettant d'isoler les sauvegardes du reste du réseau.
- Pour cela il convient de prendre contact avec nos services d'ingénierie réseau qui sauront analyser votre infrastructure et vous proposer les solutions adaptées.

COMMENT REAGIR EN CAS D'INFECTION

1°) Déconnecter immédiatement les appareils infectés de tout réseau filaire ou Wifi : cela empêchera le Cryptolocker de communiquer avec son serveur C&C(command and control) et évitera le chiffrement.

Nous vous conseillons de débrancher immédiatement électriquement votre poste de travail.

2°) Déconnecter immédiatement le Routeur du réseau Internet

3°) Appeler immédiatement nos services d'assistance

4°) Ne pas payer la rançon.

5°) Contacter la gendarmerie et la CNIL

6°) Contacter son assurance

Clauses des contrats d'assurance Cyber :

5. **DISPOSER** de logiciels anti-virus, anti-malware et pare feu ainsi que PROCÉDER à une mise à jour régulière de l'ensemble de ses dispositifs informatiques, de ses serveurs et réseaux, notamment pour les mises à jour de sécurité conformément aux recommandations de ses fournisseurs informatiques;
6. **DISPOSER** de procédures de sauvegarde hebdomadaire sur des équipements déconnectés et/ou externalisés :

(Extrait contrat d'assurance Cyber Risques)

VOS OBLIGATIONS EN CAS DE PIRATAGE

- Prévenir la CNIL dans le cadre de la Législation Européenne RGPD
- La CNIL vous demandera d'informer tous les contacts personnels impactés par le piratage sous 72 H.
- https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

EXISTE-T-IL UNE PROTECTION EFFICACE ?

Il n'existe pas (à notre connaissance) une solution efficace mais une somme de solutions permettant de minimiser le risque.

Nous conseillons vivement en 1er lieu de réaliser un Audit Cyber Sécurité afin de cartographier le système d'information et ses vulnérabilités.

Espace Technologie compte dans son effectif un spécialiste en cyber sécurité

- Nous sommes très peu d'entreprises informatiques en France, (encore moins dans l'ouest) à posséder ce type de compétence, car la grande majorité des diplômés rejoignent les équipes de cyber Défense de l'armée.

PROFIL DE NOTRE RESPONSABLE SECURITE DES SYSTEMES D'INFORMATIONS

Doublement diplômé en Cyber sécurité

- **Mastère spécialisé cyber sécurité à Centrale Supélec (Bac + 6)**
  - L'école Française la plus reconnue en Cyber Sécurité

- Ce mastère spécialisé a été classé 1er dans la catégorie « Télécoms, réseaux et sécurité des systèmes » du classement SMBG 2019
- Label "Cyber Excellence" par le ministère de la défense

- **Mastère spécialisé cyber sécurité à IMT Atlantique**

  - Préparation Norme ISO 27001
  - Ingénieur Système et réseau

Parcours professionnel

- Ingénieur système spécialisé dans les systèmes Windows/Linux et réseau(Firewall).
- Passionné de cyber sécurité et formé aux dernières générations d'attaques cyber criminelles

- Depuis 2019 : Responsable Sécurité et cyber surveillance chez Espace Technologie
- De 2015 à 2019 : Espace Technologie en qualité d'ingénieur système et réseau.
- De 2013 à 2015 : Administrateur Système Linux chez un fournisseur d'accès Internet.

Une fois l'audit réalisé les actions à mener vous seront conseillées

Plus d'informations sur nos prestations contactez-nous :

ESPACE TECHNOLOGIE
Parc d'Activités Schweitzer
26 rue du Bois Fossé - BP 147
85301 CHALLANS Cedex
Tél. 02 51 49 31 31

www.espace-technologie.com
contact@espace-technologie.com